UTAH DEPARTMENT OF HEALTH HIPAA PRIVACY POLICY

PURPOSE

This policy applies only to covered programs (CP) within the Utah Department of Health. It outlines general guidelines and expectations for the necessary collection, use, and disclosure of health information about clients in order to provide services and benefits to clients while maintaining reasonable safeguards to protect the privacy of their information.

COMPLIANCE WITH HIPAA PRIVACY REGULATION

A CP may not use or disclose protected health information (PHI) except as allowed by the HIPAA regulations. This policy covers the most common circumstances where a CP may use or disclose PHI. If this policy does not explicitly allow a use or disclosure, the CP must obtain permission from the CP's privacy officer prior to using or disclosing PHI.

DEFINITIONS

"Client" means an individual who receives or has received benefits or services from a covered program, including deceased individuals.

"Covered program" or "CP" means the Division of Health Care Financing, Children's Health Insurance Program, Primary Care Network, Health Clinics of Utah, and Family Dental Clinics and any other program that the executive director designates as a covered program.

"Disclose" means to release orally or in writing any protected health information outside of the covered programs within the Department.

"Plan" means the Division of Health Care Financing, Children's Health Insurance Program, Primary Care Network

"Provider" means Health Clinics of Utah, and Family Dental Clinics.

SAFEGUARDING CONFIDENTIAL INFORMATION ABOUT CLIENTS.

(1) CPs may collect, maintain, use, transmit, share, and disclose information about clients to the extent needed to administer the CP's programs, services and activities.

(2) Each CP will safeguard all confidential information about clients, inform clients about the CPs' privacy practices and respect client privacy rights, to the full extent required under this policy.

COMPLAINTS

(1) Client complaints regarding treatment of PHI shall be directed to the CP's privacy officer.

(2) A CP may not intimidate, threaten, coerce, discriminate against, or take any action against any person for exercising any right afforded by HIPAA, including filing complaints, participating in HIPAA enforcement investigations, and opposing any action made unlawful by HIPAA.

(3) A CP may not require a client to waive any of the client's rights under HIPAA as a condition of the provision of treatment, payment, enrollment in a plan or eligibility for benefits.

ROUTINE AND RECURRING DISCLOSURES

(1) Routine and recurring disclosures are disclosure that are compatible with the purposes for which information is collected.

(2) For routine and recurring disclosures of records outside the CP, without the authorization of the client a CP shall:

(a) Determine who is requesting the information and the purpose for the request;

(b) If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "non-routine use" procedures in the following section.

(c) review the client's record and assure that the PHI that is disclosed is limited to that reasonably necessary to achieve the purpose of the disclosure.

(d) Confirm that the applicable CP policies and program rules permit the requested use, and that the nature or type of the use is routine and recurring for the CP;

(e) Identify the kind and amount of information that is necessary to respond to the request;

(f) If the disclosure is one that must be included in the CP's accounting of disclosures, include required documentation in the accounting log; and

(g) not disclose a client's entire medical record unless the request specifically justifies why the entire medical record is needed.

(3) The following identifies several examples of uses and disclosures that are compatible with the purposes for which information is collected:

(a) disclosures required by law, such as mandatory child abuse report, disease reporting, Medicaid Fraud;

(b) disclosures to public health agencies as permitted under HIPAA and state law; and

(c) disclosures to assistant attorneys general for the purpose of obtaining its advice and legal services.

NON-ROUTINE DISCLOSURES

(1) A "non-routine disclosure" is a disclosure of records outside a CP that is not for a purpose for which it was collected.

(2) For non-routine disclosures, DHS clusters and program areas shall:

(a) Determine who is requesting the information and the purpose for the request;

(b) If the request **is** compatible with the purpose for which it was collected, apply the "routine and recurring disclosure" procedures in the previous section.

(c) Determine which information of the client is within the scope of the request, and what CP policies and program rules apply to the requested use;

(d) If the information requested can be disclosed under the applicable program and HIPAA policies, limit the amount of information to the minimum amount necessary to respond to the request;

(e) not disclose a client's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor.

(f) document the disclosure in the accounting log.

(3) CP staff shall review requests for non-routine disclosures on an individual basis.

MINIMUM NECESSARY INFORMATION

(1) Each CP will use or disclose only the minimum amount of information necessary to provide services and benefits to clients, and only to the extent provided in Utah Department of Health HIPAA policies.

(2) This policy does not apply to:

(a) disclosures to or requests by a health care provider for treatment;

(b) uses or disclosures made to the client;

(c) uses or disclosures authorized by the client;

(d) disclosures made to the Secretary of the United States Department of Health and Human Services in accordance with federal HIPAA regulations at 45 CFR 160, Subpart C;

(e) uses or disclosures that are required by law; and

(f) uses or disclosures that are required for compliance with federal HIPAA regulations at 45 CFR, Parts 160 and 164.

(3) When using or disclosing an client's information, or when requesting an client's information from a provider or health plan, a CP's employees must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

(4) A CP shall honor public health requests as if the request is for the minimum necessary information.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

CP staff must take reasonable steps to safeguard confidential information from any intentional or unintentional use or disclosure.

DISCLOSURES AUTHORIZED BY THE CLIENT

(1) A CP may use or disclose PHI pursuant to and in compliance with a HIPAA compliant consent or authorization that has been approved by the CP's privacy officer

(2) A CP must check each authorization to verify that it meets the HIPAA authorization requirements.

USES AND DISCLOSURES FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS

(1) A CP may use and disclose PHI without consent or authorization to carry out its own treatment, payment, or health care operations.

(2) A CP may disclose PHI without consent:

(a) for treatment activities of another health care provider.

(b) to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(c) if the client was a patient of the CP and the other covered entity, the CP may release to the other covered entity for quality improvement or peer review or for health care fraud and abuse detection or compliance.

(d) to other CPs within the Department as necessary to provide services to the client

DISCLOSURES PERMITTED BY LAW

HIPAA allows for many other disclosures. Listed below are some disclosures that may be made after consulting with the CP's privacy officer. The CP's privacy officer shall follow the HIPAA regulations in determining whether to disclose and may authorize single disclosures, disclosures of a series of records, or disclosures or a defined type. The privacy officer's authorization to disclose must be documented in writing. The other disclosures include disclosures:

(1) to public health authorities;

(2) to persons involved with FDA monitoring of drugs;
(3)to comply with abuse, neglect, domestic violence, and injury reporting laws;
(4) for administrative or judicial proceedings;
(5) to comply with law enforcement investigations
(6) to avert a serious threat to the health or safety individuals;
(7) to funeral directors;
(8) to organ procurement organizations;
(9) to health oversight agencies; and
(10) for research purposes.

REQUIRED DISCLOSURES

(1) A CP must disclose PHI if the disclosure is required by law. Authorization of the client is not required for disclosures required by law. Disclosures required by law must be limited to the relevant requirements of the applicable law. These include disclosures to report:

(a) child or elder abuse or neglect;
(b) domestic violence;
(c) injuries;
(d) communicable diseases and other public health reporting required by law; and
(f) other reporting required by statute or rule.

(2) A CP must immediately notify its privacy officer if it discloses PHI for reporting of child or elder abuse, domestic violence, and injuries.

SPECIAL RULES FOR MENTAL HEALTH RECORDS

CP staff must clear the release of psychotherapy records with the CP's privacy officer.

FAMILY AND RESPONSIBLE PERSONS

A CP may disclose PHI to family and persons responsible for or assisting in the health care of the client, as follows:

(1) to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to the person's involvement with the client's care or payment related to the client's health care;

(2) to notify family, relatives or the client's responsible individual of the client's location, general condition, or death if it is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the client's health care;

(3) a CP may use professional judgment and its experience with common practice to make reasonable inferences of the client's best interest in allowing a person to act on behalf of the client to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI;

(4) if the client is present or readily available, a and the CP

(a) obtains the client's oral or written agreement;

(b) provides the client with the opportunity to object to the disclosure, and the client does not express an objection; or

(c) reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure;

(5) to guardians;
(6) persons acting in loco parentis for the client's health care; and
(7) personal representatives of the client's estate.

EMERGENCIES

(1) A provider may, without prior consent, use or disclose PHI created or received under paragraph to carry out treatment, payment, or health care operations :

(a) In emergency treatment situations, if the provider attempts to obtain such consent as soon as reasonably practicable after treatment;

(b) If the provider is required by law to treat the individual, and the provider attempts to obtain consent but is unable to obtain consent; or

(c) If the provider attempts to obtain consent from the individual but is unable to obtain consent due to substantial barriers to communicating with the individual, and the provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.

(2) A provider that fails to obtain such consent must document its attempt to obtain consent and the reason why consent was not obtained.

DISASTERS

A CP may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, to coordinate with such entities in notifying family, relatives or the client's responsible individual of the client's location, general condition or death.

BUSINESS ASSOCIATES

(1) A business associate is a person, other than an employee that performs, or assists in the performance of:

(a) A function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(b) Any other function or activity regulated by 45 CFR Part 164, Subpart E; or

(c) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a CP, or to or for an organized health care arrangement in which the CP participates, where the provision of the service involves the disclosure of individually identifiable health information from a CP or organized health care arrangement, or from business associate of either of them.

(2) A CP may disclose PHI to a business associate only if it has in place a HIPAA-compliant business associate contract or has received specific instruction otherwise from the privacy officer.

(3) A CP may enter into a business associate contract only after it has been approved by the CP's privacy officer.

MANDATORY AUTHORIZATIONS, REVOCATIONS

(1) A provider may condition treatment and a plan may condition enrollment upon obtaining authorization from the client to use and disclose PHI as necessary to carry out treatment, payment, and health care operations.

(2) To the extent that a CP has not relied on it a client may revoke an authorization at any time by providing a written notice to the CP.

AUTHORIZATIONS

(1) For uses and disclosures other than for treatment, payment, and health care operations or as specifically allowed in this policy, a CP must obtain an authorization to use or disclose PHI.

(2) A CP must use a HIPAA-compliant authorization that has been approved by the CP's privacy officer when:

(a) requesting PHI from another CP or covered entity.

(b) requesting authorization from its client for its own uses and disclosures.

(3) If a CP obtains an authorization from a client, the CP must provide a copy of the authorization to the client.

(4) An authorization that a CP receives to allow it to disclose PHI must meet all of the following requirements:

(a) The authorization must be in plain language.

(b) The authorization must contain all of the following:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s), or class of persons, to whom the CP may make the requested use or disclosure;

(iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

(v) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

(vi) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;

(vii) Signature of the individual and date; and

(viii) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

(c) The authorization must not be expired as provided in the authorization.

DE-IDENTIFIED INFORMATION

(1) A CP may use and disclose de-identified information without restriction.

(2) A CP must verify with the CP's privacy officer that the information meets the HIPAA requirements for de-identification.

NOTICE OF PRIVACY PRACTICES

A notice of privacy practices must be first approved by the plan's privacy officer and comply with HIPAA requirements.

(1) A plan must provide to clients and any other person upon request a notice of privacy practices.

(2) A plan must provide the notice to its clients:

(a) at the time of enrollment; and

(b) within 60 days of a material revision to the notice.

(3) A plan must notify its clients at least once every three years of the availability of the notice and how to obtain the notice.

(4) A provider that has a direct treatment relationship with a client must provide the notice

to each client no later than the date of the first service delivery, including service delivered electronically, after April 14, 2003

(5) If the provider maintains a physical service delivery site, the provider must:

(a) have its current notice available at the service delivery site for individuals to request to take with them; and

(b) post the current notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice; and

(6) A CP that issues a notice in conjunction with another CP or other covered entity must first obtain the approval of the CP's privacy officer.

REQUESTS FOR PRIVACY PROTECTIONS

(1) A CP's client may request in writing that the CP restrict uses and disclosures of PHI concerning the client.

(a) A CP must refer all requests for restriction to the CP's privacy officer.

(b) A CP may refuse the restriction.

(c) A CP that agrees to a restriction may not use or disclose PHI in violation of the restriction, except that, if the client who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the CP may use the restricted PHI, or may disclose it to a health care provider, to provide treatment to the client.

(d) If restricted PHI is disclosed to a health care provider for emergency treatment, the CP must request that the health care provider not further use or disclose the information.

(2) A CP desiring to terminate its agreement to a restriction shall consult with the CP's privacy officer prior to terminating the restriction

CONFIDENTIAL COMMUNICATIONS

A CP must accommodate reasonable requests by clients for confidential treatment of PHI.

(1) A provider's client may request in writing to receive communications of PHI from the provider by alternative means or at alternative locations.

(2) A plan's client may request in writing to receive communications of protected health information from the plan by alternative means or at alternative locations, if the client clearly states that the disclosure of all or part of that information could endanger the client.

(3) A CP may condition the provision of a reasonable accommodation on:

(a) When appropriate, information as to how payment, if any, will be handled; and

(b) Specification of an alternative address or other method of contact.

(4) A provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

CLIENT RIGHT TO ACCESS INFORMATION

(1) Upon submitting a written request, a client has a right to access PHI about the client. A CP must respond to a client's request within 30 days, granting or denying access. If the CP cannot respond within 30 days, the CP must notify the CP's privacy officer prior to the expiration of the 30 days.

(2) A CP may deny access to the following without providing an opportunity for appeal:

(a) psychotherapy notes

(b) information compiled for litigation, including administrative hearings

(c) research information while the research is ongoing

(d) information collected from a party other than a health care provider with the promise of confidentiality, if allowing the client to access the information would reveal the source of the information.

(3) A CP may deny access to the following circumstances, but must provide an opportunity for appeal:

(a) information that a licensed health care professional has determined, in the exercise of professional judgment, is reasonably likely endanger the life or physical safety of the client or another individual;

(b) the PHI make reference to another individual (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access would is reasonably likely to cause substantial harm to the other individual; and

(c) the request for access is made by a client's personal representative and information a licensed health care professional has determined, in the exercise of professional judgment, that the access would is reasonably likely to cause substantial harm to the individual or another person.

(4) If a client appeals a denial of access to information, the CP must refer the appeal to the privacy officer.

(5) If a CP provides a client access to PHI, the CP must allow the client to inspect and take a copy of the PHI.

(6) If the client requests the PHI in a specific format, the CP must provide it in the requested format if it is readily producible in that format

(7) A CP may provide a summary of the PHI if the client agrees in advance.

(8) A CP may and charge for the summary if the client agrees in advance.

(9) A CP may charge for summary costs if the client has agreed to summary costs and a reasonable cost-based fee for copies, labor to copy, and mailing.

(10) If a CP denies access to all or part of a client's PHI, the CP must notify the CP's privacy officer who will notify the client of the denial and the client's rights to appeal.

(11) If a CP does not maintain the PHI requested by the client but knows where the PHI is maintained, the CP must inform the client where the PHI is located.

AMENDMENT OF PHI

A client may seek amendment of PHI maintained by a CP. A request for amendment must be in writing. If a client seeks an amendment, the CP must refer the request to the CP's privacy officer.

ACCOUNTING OF DISCLOSURES

(1) A client may request an accounting of disclosures made by a CP. The request for the accounting must be in writing. If a client seeks an accounting, the CP must refer the request to the CP's privacy officer.

(2) Each CP must document the following disclosures at the time of disclosure:

(a) date of the disclosure;

(b) the name of the person or entity that received the PHI, and the address if available;

(c) a brief description of the information disclosed;

(d) a brief statement of the purpose of the disclosure that reasonably infomrs the individual of the basis for the disclosure, or a copy of the request from the client or from the person requesting a disclosure permitted or required by law.

(3) If there have been multiple disclosures to the same person or entity under a single

request, the CP need only record the date and the frequency, periodicity, or number of disclosures for disclosures after the initial disclosure.

(4) A CP shall contact the privacy for instructions on documenting disclosures for research purposes.

(5) The privacy officer must document and retain the accounting of disclosures

DOCUMENTATION

A CP must document and retain the following for six years:

(1) authorizations and consents to use or disclose PHI;

(2) agreements for special confidential communications or privacy protections;

(3) information necessary to account for disclosures as required by this policy;

(4) supporting documentation establishing that a disclosure is of de-identified information; and

(5) supporting documentation for releases required or permitted by law.

CONFLICT WITH OTHER REQUIREMENTS REGARDING PRIVACY AND SAFEGUARDING

(1) The Department of Health has adopted reasonable policies and procedures for administration of its programs, services and activities. If any state or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any Department of Health policy regarding the privacy or safeguarding of information, the Department of Health shall act in accordance with that stricter standard.

(2) CP staff shall act in accordance with established CP policy and procedures regarding the safeguarding and confidentiality of client health information in all CP programs, services and activities.

(3) In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, the CP employee will seek guidance from the CP privacy coordinator.